POLITIQUE GENERALE DE LA SECURITE ET DE LA PROTECTION DES DONNEES A LA CRAMIF

DOCUMENT PUBLIC

15 Novembre 2021

PUBLIC

Page

1 Présentation du document et enjeux

L'Assurance Maladie a une mission de service public, elle est l'assureur santé obligatoire des salariés qui relèvent du régime général. A ce titre :

- elle détient un patrimoine informationnel unique et stratégique dont un grand nombre de données personnelles. Elle a donc des responsabilités particulières, dont certaines sont explicitement mentionnées dans le Règlement général sur la protection des données (RGPD).
- elle met en œuvre son propre Système d'Information qui intègre l'ensemble des ressources humaines, informatiques, matérielles et immobilières mises en œuvre pour les traitements. Ce système d'information est sécurisé.

Ce document présente la politique de sécurité et de protection des données de la CRAMIF. Notre objectif est que toute personne en relation avec la CRAMIF soit toujours pleinement informée des catégories d'informations que nous recueillons, de la manière dont nous les utilisons, et des circonstances dans lesquelles elles peuvent être communiquées ou corrigées.

2 Le contexte applicable

Le contexte applicable à la sécurité mise en œuvre à la CRAMIF est rattaché depuis le 25 mai 2018 aux exigences du Règlement Européen 2016/679 du 27 avril 2016 (RGPD).

En France, la loi informatique et liberté (Loi n°78-17) du 6 janvier 1978 a fait l'objet d'un processus de mise en conformité avec le RGPD qui s'est achevé par le décret de mise en application du 29 mai 2019.

Par ailleurs, en 2019, l'organisme doit s'adapter à une nouvelle Politique de Sécurité des Systèmes d'Information (PSSI) Assurance Maladie, alignée sur la PSSI du Ministère chargé des Affaires Sociales (MCAS).

Protection des données personnelles

L'article 4 du RGPD définit les concepts suivants :

- *« données à caractère personnel toute information se rapportant à une personne physique identifiée ou identifiable (personne concernée) ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, tel un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.*
- *« traitement », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion, toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.*
- *« fichier » tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.*

La PSSI : Politique de Sécurité du Système d'Information

La Politique de Sécurité du Système d'Information (PSSI) vise à définir les mesures à mettre en œuvre afin de contenir les risques pesant sur le Système d'Information (matériels, logiciels, information traitée, ressources humaines, organisations, infrastructures - sites, locaux).

Elle s'organise à travers les éléments suivants :

- organisation,
- gestion des biens,
- ressources humaines,
- ressources physiques (matériels),
- exploitation et télécommunications,
- contrôles d'accès,
- applications,
- incidents,
- plan de continuité d'activités,
- conformité.

La SSI prend en compte :

- la sécurité des personnes, des biens et des informations (vol de matériel ou de documents, incendie, coupure de courant, occupation de locaux…)
- la sécurité des données et des applications en garantissant l'intégrité, la disponibilité et la confidentialité à un niveau d'exigence élevé,
- la sécurité du matériel pour assurer la disponibilité et un niveau de contrôle d'accès adapté.

3 Le rôle et les responsabilités de chacun des acteurs concernés par la protection de données personnelles

Le Directeur Général de la CRAMIF est le Responsable de Traitement au sens du RGPD :

- il définit (par l'intermédiaire des différents responsables), la ou les finalité(s) pour chaque traitement et les moyens mis en œuvre.
- conformément aux dispositions édictées par les articles 24 et suivants du RGPD, il est responsable en cas de non-respect des règles applicable à la protection des données personnelles.

Le MSSI (Manager de la Sécurité des Systèmes d'Information) a la responsabilité de veiller au respect des mesures de sécurité nécessaires à la protection des données :

- il procède à l'analyse de risques concernant la Sécurité du Système d'Informations pour chaque déclaration ou modification de traitement, et fait des préconisations,
- il est informé de tous les incidents, failles de sécurité ou violations de données, suit leur résolution et participe à la revue périodique des incidents de sécurité.

Le Délégué à la Protection des Données (DPO : Data Protection Officer), veille de manière indépendante à la protection des données personnelles et au respect de la loi informatique et libertés (article 38 du RGPD) :

- il informe et conseille le responsable de traitement, l'ensemble des services, ainsi que les agents sur les évolutions règlementaires relatives à la protection des données,
- il accompagne la mise en œuvre des traitements de données personnelles, et à cette occasion formule les conseils et les recommandations nécessaires au respect de la loi informatique et libertés,
- il contrôle le respect du RGPD, la répartition des responsabilités et les audits s'y rapportant en apportant son aide dans l'analyse des traitements,
- il tient le registre des activités de traitement et met à jour la liste des traitements (registre ou cartographie)
- il répond aux demandes des personnes concernées et communique les informations appropriées
- il est tenu informé de toute demande ou réclamation portant sur le traitement des données personnelles,
- il informe et sensibilise le personnel aux enjeux de la protection des données,

- il alerte le responsable des traitements sur l'existence de manquements à la loi Informatique et Libertés,
- il est la personne référente pour toute alerte violation de données car il maîtrise la procédure articulée autour de l'information de la MEC CNAM, de l'information de la CNIL (déclaration à effectuer en ligne) et de l'information des personnes concernées.
- il rédige et remet au responsable des traitements un bilan annuel des actions menées.

Et en cas de contrôle par la CNIL :

- il est associé aux échanges,
- il reçoit la copie du procès-verbal et est informé des suites données,
- il reçoit le cas échéant la copie du rapport à des fins de sanction dans le cadre de poursuites,
- il est consulté pour la rédaction des observations en réponse.

4 L'engagement du Directeur Général de la CRAMIF

En 2005, le Directeur Général avait déjà désigné le Manager de la Sécurité du Système d'Informations (MSSI) de la CRAMIF en application de la PSSI nationale. En 2013, il lui a confié le pilotage de l'ensemble des actions conduisant à la mise en œuvre de la PSSI, avec une confirmation en 2014 par lettre de mission

Depuis 2018, les exigences du RGPD ont été intégrées progressivement dans le droit français, la fonction de délégué à la protection des données (DPO) s'est élargie.

Une lettre de mission a été rédigée le 14 mars 2018 afin d'établir le cadre de la cette fonction. Le Directeur général désigne auprès de la CNIL, conformément au RGPD, l'identité du DPO. La nouvelle DPO a été enregistrée par la CNIL le 30/10/2021.

Avec ces désignations, le Directeur Général s'engage et soutient la mise en œuvre des actions qui concourent à la sécurité et à la protection des données.

En 2017, le Directeur Général a souhaité formaliser spécifiquement son engagement quant à la Politique Générale de Sécurité des données et procède au renouvellement de cet engagement en 2021.

Lettre d'engagement du Directeur Général de la CRAMIF

Dans le cadre de la politique de gestion des données à caractère personnel, le Directeur Général engage la CRAMIF sur le respect des dix principes suivants :

Principe 1 – Responsabilité

L'organisme est responsable des traitements de données à caractère personnel qu'il met en œuvre directement ou indirectement en France et à l'étranger. En conséquence, il se conforme aux réglementations applicables, en particulier à la loi informatique et libertés modifiée et au RGPD.
Il accomplit toutes les formalités nécessaires pour assurer la conformité au RGPD des traitements de données à caractère personnel.

Principe 2 – Détermination des finalités de la collecte de données à caractère personnel

L'organisme détermine les finalités pour lesquelles il recueille des données à caractère personnel. Ces finalités doivent être légitimes et respectées pendant la durée de vie du traitement.

Principe 3 – Transparence et licéité de la collecte

L'organisme s'engage à ne traiter que les données à caractère personnel pour lesquelles il aura obtenu le consentement explicite de la personne concernée ou, comme le lui autorise le RGPD, les données dont le traitement est nécessaire à l'exécution de sa mission d'intérêt public.
L'organisme fournit aux personnes concernées, les informations sur la finalité du traitement, l'identité et les coordonnées du responsable du traitement, l'identité et les coordonnées de la Déléguée à la Protection des données, l'étendue de leurs droits.

Principe 4 – Limitation de la collecte des données à caractère personnel.
L'organisme se limite au recueil des seules données à caractère personnel nécessaires à l'atteinte des finalités énoncées.

Principe 5 – Limitation de la conservation des données à caractère personnel
L'organisme veille à la mise à jour des données personnelles qu'il traite tout en respectant les finalités visées. Les durées de conservation ne doivent pas excéder celles nécessaires à l'atteinte des finalités visées.

Principe 6 – Sécurité physique et logique des données à caractère personnel
L'organisme détermine et met en œuvre les moyens nécessaires à la protection des systèmes de traitement de données à caractère personnel pour éviter toute intrusion malveillante et prévenir toute perte, altération ou divulgation de données à des personnes non autorisées.
L'organisme détermine et met en œuvre des mesures de sécurité permettant de garantir la confidentialité des données.
L'organisme exige de ses sous-traitants qu'ils présentent des garanties suffisantes pour assurer la sécurité et la confidentialité des données à caractère personnel.

Principe 7 – Accès aux données à caractère personnel – information
L'organisme met en œuvre les moyens nécessaires pour informer toute personne de l'existence de données personnelles qui la concernent et de l'usage qui en est fait.
Il met en œuvre les moyens nécessaires pour garantir aux usagers l'accès aux données à personnelles qui les concernent lorsqu'ils en font la demande. Il prend toute mesure pour rectifier ou supprimer les informations erronées.

Principe 8 – Communication et mise en œuvre de la politique de gestion des données à caractère personnel.
L'organisme met à disposition de ses usagers une information claire et transparente sur la politique de gestion des données à caractère personnel et les principes qui la gouvernent.
L'organisme détermine et met en œuvre l'ensemble des mesures opérationnelles utiles et nécessaires pour permettre à ses services d'appliquer les principes de la politique de gestion des données à caractère personnel.

Principe 9 – Respect des principes énoncés.

L'organisme est pourvu d'une Déléguée à la Protection des Données qui veille au respect des règles en matière de collecte et de traitement de données personnelles, énoncées dans le présent document.

Toute personne doit pouvoir saisir la Déléguée à la Protection des Données(DPO) sur les principes énoncés ci-dessus.

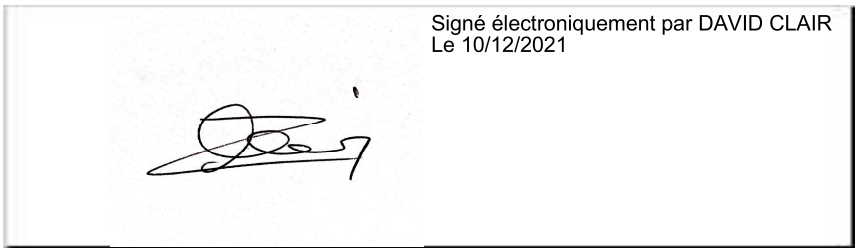
Principe 10 – Pérennité de la politique de gestion des données à caractère personnel

Pour les besoins de la pérennité de sa politique de gestion des données à caractère personnel, l'organisme s'assure régulièrement de l'adéquation des principes qui la composent aux évolutions des technologies, du droit et des besoins des usagers et des tiers.

Paris,

Le Directeur Général

Signé électroniquement par DAVID CLAIR
Le 10/12/2021



5 Les engagements de la CRAMIF

Au-delà de l'engagement aux 10 grands principes énoncé précédemment, la CRAMIF souhaite s'engager en matière de conformité sur la protection des données et sur la sécurité mise en place conformément à la PSSI, à travers plusieurs dispositifs complémentaires que nous vous présentons dans ce chapitre.

5.1 Non-communication des données personnelles

Vos Données personnelles ne seront jamais vendues, partagées ou communiquées à des tiers, en dehors des cas prévus par la Loi.

Vos données personnelles pourront toutefois être communiquées à des tiers agissant pour notre compte dans le cadre d'un traitement spécifique conformément aux finalités pour lesquelles nous sommes dépositaires. Elles seront traitées suivant la réglementation en vigueur. Ces tiers sont liés par contrat à n'utiliser vos données personnelles qu'aux fins convenues et à ne pas les vendre ou les divulguer à d'autres tiers sauf si la loi le requiert et si nous les y autorisons explicitement.

5.2 Sécurité des locaux, des biens, et des personnes.

Les locaux de la CRAMIF sont disposés en plusieurs points géographiques, tous situés en région Ile de France.

Pour les locaux situés avenue de Flandre et place de l'Argonne, La CRAMIF, établissement recevant du public, s'engage à mettre en œuvre l'ensemble des dispositions légales visant à assurer la sécurité des locaux, des biens, et des personnes. Ces deux sites disposent d'un PC sécurité permettant de prendre en charge les interventions d'urgence.

Pour ses centres externes hébergés dans des locaux de l'Assurance Maladie, la PSSI de l'Assurance Maladie s'applique, avec les mêmes exigences.

5.3 Cookies Internet

Notre site internet utilise Google Analytics. En navigant vous nous autorisez à utiliser des cookies à des fins de mesures d'audience. Les services de mesures d'audience permettent de mesurer le nombre de visites, le nombre de pages vues, ainsi que l'activité des visiteurs sur le site et leur fréquence de retour.

Vous pouvez refuser l'utilisation de Google Analytics directement depuis le site.

5.4 Liens vers d'autres sites

La présente Politique de protection des données s'applique uniquement à notre site, et pas aux sites Web détenus par nos partenaires. Nous donnons parfois des liens vers d'autres sites Web que nous jugeons susceptibles d'intéresser nos visiteurs.

Pour tout accès à votre compte assuré depuis notre site, vous serez redirigé sur le site AMELI de l'Assurance Maladie.

Cette politique est diffusée en interne auprès des salariés via l'intranet et en externe via le site internet Cramif.fr.

Paris,
La DPO

Signé électroniquement par Sophie BETERMIEZ Le 10/12/2021

6 Glossaire de la sécurité

Confidentialité : caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.

Disponibilité : aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances.

Intégrité : garantit que les informations traitées ne sont modifiées que par une action volontaire et légitime.